Indian Institute of Technology Kanpur

Proposal for a New Course

1. Course No: CS675

2. Course Title: Cryptography for Cybersecurity

3. Per Week Lectures: 3(L), Tutorial: 0 (T), Laboratory: 0 (P), Additional Hours [0-2]: 0 (A), **Credits (3-0-0-0-9)**: **Duration of Course: Full semester**

4. Proposing Department: Computer Science and Engineering

i) Other Departments/IDPs which may be interested in the proposed course: Mathematics, Electrical Engineering: Wadhwani School of Advanced AI & Intelligent Systems

ii) Other faculty members interested in teaching the proposed course: Somitra Sanadhya

5. Proposing Instructor(s): Angshuman Karmakar (angshuman@iitk.ac.in)

7. Course Description:

A) Objectives: This course is designed to give students a comprehensive understanding of cryptographic protocols that lies behind different methods used in cybersecurity.

Students will master key concepts such as secure system design, cryptographic techniques, authentication and access models, secure communications, digital forensics, and emerging technologies.

Emphasis is placed on the ability to analyze threats, evaluate and apply appropriate protocols, ensure data integrity, and adapt to new developments in the field.

By the end of the course, students will be equipped to evaluate, design, and implement secure solutions and critically respond to security challenges in real-world environments.

B) Contents (preferably in the form of 5 to 10 broad titles):

Lecture-wise break-up (considering the duration of each lecture is 50 minutes)

Serial	Broad title	Topics	No of lectures
1	Introduction: Cybersecurity Mechanisms and Cryptography	• Cybersecurity overview: definitions, goals (confidentiality, integrity, availability) • Threat landscape: common attack types (malware, phishing, APTs, DoS, insider threats) • Types of controls: preventive, detective, corrective • The role of cryptography in security mechanisms • Brief introduction to cryptographic protocols and primitives	6

		• Roadmap of the course modules and expectations	
2	Authentication and Access Management	• Entity Authentication I (Principles and Passwords) • Entity Authentication II (Biometrics, MFA, Zero-Knowledge) • Cryptography in Entity Authentication (Protocols) • Access & Identity Management I (Access Models) • Access & Identity Management II (Single Sign-On, OAuth, SAML) • Cryptography in Access Management (PKI, Certificates)	8
3	Secure Tunneling and Communications	• Intrusion Detection Systems I (Theory & Types) • Intrusion Detection Systems II (Cryptographic Techniques) • Secure Tunneling I (VPN Concepts) • Secure Tunneling II (IPSec, SSL/TLS, SSH) • Secure Communications I (HTTPS, Email Crypto) • Secure Communications II (TLS, Modern Messaging Protocols) • Secure Wireless Communication	6
4	Password Management	• Password Management I (Fundamentals) • Password Management II (Advanced)	4
5	Digital Forensics and Log Integrity	• Data Integrity & Digital Signing I (Checksums, MAC) • Data Integrity & Digital Signing II (Signatures, PKI) • Digital Forensics & Log Integrity • Blockchain & Distributed Ledger Security	4
6	Notarization and Trusted Third Parties	• Trusted Third Parties (TTPs): CA infrastructure, notaries, timestamping authorities • Digital certificates and trust chains	3

		• Blockchain-based notarization: proof-of-existence, document anchoring • Legal and practical considerations in digital notarization	
7	Software Update and Code Signing	• Secure software update architectures (signed updates, update chain of trust) • Code signing process and certificate management • Supply-chain attack scenarios and defenses • Timestamping and update validation	3
8	Emerging Mechanisms & Protocols	• Post-quantum cryptography: rationale, status, candidate algorithms • Zero-trust security models and architecture • Federated and decentralized identity (DID, verifiable credentials) • AI and machine learning in threat detection, automated response and resilience • Cloud and IoT security protocols: unique challenges	6

C) Recommended pre-requisites, if any: Mandatory: algorithms, programming knowledge
Desirable: Basic knowledge of cryptography
D) Short summary for including in the Courses of Study Booklet: This course provides a rigorous treatment of cybersecurity mechanisms and cryptographic protocols. This course is into six modules: cryptographic foundations; authentication and access management; secure tunneling and communications; password management; forensics and log integrity; and emerging mechanisms and protocols.

Students will learn to design and analyze secure systems using symmetric and asymmetric encryption, hash functions, digital signatures, and key-exchange protocols; implement and evaluate authentication frameworks (passwords, multifactor, zero-knowledge proofs, PKI, OAuth, SAML); deploy VPNs, TLS/SSL, SSH, and secure wireless networks; and apply integrity checks, secure logging, and digital forensics techniques.

The course also addresses some advanced techniques such as blockchain and distributed ledger security, post-quantum cryptography, zero-trust

architectures, privacy-enhancing technologies, intrusion detection techniques, etc. This course will prepare the students graduates for technical roles in security architecture, incident response, and research.

7. Recommended text/reference books:

i) A Graduate Course in Applied Cryptography. Dan Boneh and Victor Shoup
ii) Understanding PKI: Concepts, Standards, and Deployment Considerations, Carlisle Adams, Steve Lloyd
iii) Cryptography and Network Security Principles and Practice, William Stallings
iv) Bitcoin and Cryptocurrency Technologies, Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder
v) Wireless Communications & Networks, William Stallings

8. Any other remarks: None

Dated: 06/10/2025

Proposer: Angshuman Karmakar

The course is approved / not approved

Convenor, DPGC

Dated: 06-Oct-2025

Department of Computer Science and Engineering

Chairperson, SPGC

Dated:

IIT Kanpur